WHAT IS CLAIMED IS:

1. A method for sharing encrypted data region among two or more processes on a tamper resistant processor having a program and data encryption/decryption function, the method comprising:

giving a common key to each one of the two or more processes in advance;

shifting an execution mode of the tamper resistant processor to an encrypted instruction execution mode;

operating an owner process among the two or more processes to generate a shared encrypted data region valid only with respect to the common key in a process space of the owner process;

operating each client process other than the owner process among the two or more processes to map the shared encrypted data region generated by the owner process to a process space of the each client process; and

setting address information of the shared encrypted data region for each process among the two or more processes in relation to the common key in an encrypted attribute register inside the tamper resistant processor.

2. The method of claim 1, further comprising:

encrypting/decrypting data to be sent/received to/from an external memory at the tamper resistant processor by referring to information set in the encrypted attribute register inside the tamper resistant processor when the each process carries out a write/read operation with respect to the shared encrypted data region.

3. A method for sharing encrypted data region among two processes on a tamper resistant processor having a program and data encryption/decryption function, the method comprising:

(a) shifting an execution mode of the tamper resistant processor to an encrypted instruction execution mode;
(b) operating each process among the two processes to generate a hidden data region of the each process in a process space of the each process;
(c) operating the two processes to generate mutually different key pairs to be used in a key exchange and carry out the key exchange between the two processes;
(d) operating the each process to generate a common key according to the key exchange;
(e) generating a shared encrypted data region to be shared by the two processes which is valid only with respect to the common key; and
(f) storing the common key and data used in a course of the key exchange in the hidden data region of the each process.

4. The method of claim 3, wherein the step (e) operates one process among the two processes to generate the shared encrypted data region in a process space of the one process and operates another process among the two processes to map the shared encrypted data region generated by the one process to a process space of the another process.

5. The method of claim 4, further comprising:
setting address information of the shared encrypted data region for the each process in relation to the common key in an encrypted attribute register inside the tamper resistant processor.

6. The method of claim 3, wherein the step (c) operates the two processes to carry out the exchange that includes a verification of a message signature, and the step (d) operates the each process to generate the common key which is authenticated according to the verification.

7. The method of claim 3, further comprising:

encrypting/decrypting data to be sent/received to/from an external memory at the tamper resistant processor by referring to information set in the encrypted attribute register inside the tamper resistant processor when the each process carries out a write/read operation with respect to the shared encrypted data region.

8. A method for sharing encrypted data region among three or more processes on a tamper resistant processor having a program and data encryption/decryption function, the method comprising:

(a) shifting an execution mode of the tamper resistant processor to an encrypted instruction execution mode;

(b) operating an owner process among the three or more processes to generate a shared encrypted data region to be shared among the three or more processes;

(c) operating the owner process to specify a common key for the shared encrypted data region;

(d) operating the three or more processes to generate an encrypted key notification region for each client process other than the owner process among the three or more processes, the encrypted key notification region being shared only between the owner process and the each client process;

(e) operating the owner process to notify the common key to the each client process through the encrypted key notification region for the each client process;

(f) operating the each client process to map the shared encrypted data region generated by the owner process to a process space of the each client process; and

(g) setting address information of the shared encrypted data region for each process among the three or more processes in relation to the common key in an encrypted

attribute register inside the tamper resistant processor.

9. The method of claim 8, wherein the step (d) includes:

(d1) operating the each process to generate a hidden data region of the each process in a process space of the each process;

(d2) operating the owner process and the each client process to generate mutually different key pairs to be used in a key exchange and carry out the key exchange between the owner process and the each client process;

(d3) operating the owner process and the each client process to generate another common key to be used between the owner process and the each client process according to the key exchange;

(d4) generating the encrypted key notification region to be shared by the owner process and the each client process which is valid only with respect to the another common key; and

(d5) storing the another common key and data used in a course of the key exchange in the hidden data region of the each process.

10. A tamper resistant processor having a program and data encryption/decryption function and a memory that stores computer readable program codes for sharing encrypted data region among two or more processes, the computer readable program codes include:

a first computer readable program code for causing said computer to give a common key to each one of the two or more processes in advance;

a second computer readable program code for causing said computer to shift an execution mode of the tamper resistant processor to an encrypted instruction execution mode;

a third computer readable program code for causing

said computer to operate an owner process among the two or more processes to generate a shared encrypted data region valid only with respect to the common key in a process space of the owner process;

a fourth computer readable program code for causing said computer to operate each client process other than the owner process among the two or more processes to map the shared encrypted data region generated by the owner process to a process space of the each client process; and

a fifth computer readable program code for causing said computer to set address information of the shared encrypted data region for each process among the two or more processes in relation to the common key in an encrypted attribute register inside the tamper resistant processor.

11. The tamper resistant processor of claim 10, wherein the computer readable program codes further include:

a sixth computer readable program code for causing said computer to encrypt/decrypt data to be sent/received to/from an external memory at the tamper resistant processor by referring to information set in the encrypted attribute register inside the tamper resistant processor when the each process carries out a write/read operation with respect to the shared encrypted data region.

12. A tamper resistant processor having a program and data encryption/decryption function and a memory that stores computer readable program codes for sharing encrypted data region among two processes, the computer readable program codes include:

a first computer readable program code for causing said computer to shift an execution mode of the tamper resistant processor to an encrypted instruction execution mode;

a second computer readable program code for causing said computer to operate each process among the two processes to generate a hidden data region of the each process in a process space of the each process;

a third computer readable program code for causing said computer to operate the two processes to generate mutually different key pairs to be used in a key exchange and carry out the key exchange between the two processes;

a fourth computer readable program code for causing said computer to operate the each process to generate a common key according to the key exchange;

a fifth computer readable program code for causing said computer to generate a shared encrypted data region to be shared by the two processes which is valid only with respect to the common key; and

a sixth computer readable program code for causing said computer to store the common key and data used in a course of the key exchange in the hidden data region of the each process.

13. The tamper resistant processor of claim 12, wherein the fifth computer readable program code operates one process among the two processes to generate the shared encrypted data region in a process space of the one process and operates another process among the two processes to map the shared encrypted data region generated by the one process to a process space of the another process.

14. The tamper resistant processor of claim 13, wherein the computer readable program codes further include:

a seventh computer readable program code for causing said computer to set address information of the shared encrypted data region for the each process in relation to the common key in an encrypted attribute register inside the tamper resistant processor.

15. The tamper resistant processor of claim 12, wherein the third computer readable program code operates the two processes to carry out the exchange that includes a verification of a message signature, and the fourth computer readable program code operates the each process to generate the common key which is authenticated according to the verification.

16. The tamper resistant processor of claim 12, wherein the computer readable program codes further include:

a seventh computer readable program code for causing said computer to encrypt/decrypt data to be sent/received to/from an external memory at the tamper resistant processor by referring to information set in the encrypted attribute register inside the tamper resistant processor when the each process carries out a write/read operation with respect to the shared encrypted data region.

17. A tamper resistant processor a having program and data encryption/decryption function and a memory that stores computer readable program codes for sharing encrypted data region among three or more processes, the computer readable program codes include:

a first computer readable program code for causing said computer to shift an execution mode of the tamper resistant processor to an encrypted instruction execution mode;

a second computer readable program code for causing said computer to operate an owner process among the three or more processes to generate a shared encrypted data region to be shared among the three or more processes;

a third computer readable program code for causing said computer to operate the owner process to specify a common key for the shared encrypted data region;

a fourth computer readable program code for causing said computer to operate the three or more processes to generate an encrypted key notification region for each client process other than the owner process among the three or more processes, the encrypted key notification region being shared only between the owner process and the each client process;

a fifth computer readable program code for causing said computer to operate the owner process to notify the common key to the each client process through the encrypted key notification region for the each client process;

a sixth computer readable program code for causing said computer to operate the each client process to map the shared encrypted data region generated by the owner process to a process space of the each client process; and

a seventh computer readable program code for causing said computer to set address information of the shared encrypted data region for each process among the three or more processes in relation to the common key in an encrypted attribute register inside the tamper resistant processor.

18. The tamper resistant processor of claim 17, wherein the fourth computer readable program code includes:

a computer readable program code for causing said computer to operate the each process to generate a hidden data region of the each process in a process space of the each process;

a computer readable program code for causing said computer to operate the owner process and the each client process to generate mutually different key pairs to be used in a key exchange and carry out the key exchange between the owner process and the each client process;

a computer readable program code for causing said computer to operate the owner process and the each client

process to generate another common key to be used between the owner process and the each client process according to the key exchange;

a computer readable program code for causing said computer to generate the encrypted key notification region to be shared by the owner process and the each client process which is valid only with respect to the another common key; and

a computer readable program code for causing said computer to store the another common key and data used in a course of the key exchange in the hidden data region of the each process.